CLAIMS

I claim:

1. A method for making a public key digital signature on a plurality of messages in an electronic system, comprising:

    a) arranging said plurality of messages into an ordered sequence of messages,

    b) constructing a hash tree from said sequence of messages, particularly computing a value of a root node of said hash tree,

    c) preparing a private key for a digital signature operation, and

    d) performing a cryptographic signature operation with said private key upon the value of said root node,

    whereby a maker of said public key digital signature can simultaneously sign said plurality of messages.

2. The method of claim 1, wherein

    a) said hash tree is constructed with a position-dependent hash function.

3. The method of claim 1, wherein

    a) said hash tree is constructed with a salted hash function that incorporates a salt value,

    whereby an outside party need not know said salt value in advance and thus would not be able to generate a tree extension.

4. The method of claim 1, wherein

    a) the value of the leaves of said hash tree are taken as the results of a hash function applied to the values of said sequence of messages,

whereby a verifier may be able to determine that said public key digital signature was not generated as a tree extension.

5. The method of claim 1, further including

    a) performing said cryptographic signature operation with padding added to the value of said root node,

whereby a verifier can verify a signature when using a cryptographic signature scheme without message recovery.

6. A method for making a public key digital signature on an individual message from out of a plurality of messages in an electronic system, comprising:

    a) arranging said plurality of messages into an ordered sequence of messages,

    b) constructing a hash tree from said sequence of messages, particularly computing a value of a root node of said hash tree,

    c) preparing a private key for a digital signature operation,

    d) performing a cryptographic signature operation with said private key upon the value of said root node, and

    e) extracting said public key digital signature from a combination of said hash tree and from the results of said cryptographic signature operation,

whereby a verifier may be able to determine the verity of said public key digital signature against a combination comprising said individual message and a public key corresponding to said private key.

7. The method of claim 6, further including

    a) incorporating a hash tree size into said public key digital signature, said hash tree size being the number of said plurality of messages,

whereby a verifier may be able to determine that said public key digital signature was not generated as a tree extension.

8. The method of claim 6, further including

    a) incorporating a salt value into said public key digital signature,

    and wherein

    b) said hash tree is constructed with a salted hash function that incorporates said salt value,

    whereby a verifier may be able to determine that said public key digital signature was not generated as a tree extension.

9. The method of claim 6, further including

    a) performing said cryptographic signature operation with padding added to the value of said root node, and

    b) incorporating the value of said padding into said public key digital signature,

    whereby a verifier can verify a signature when using a cryptographic signature scheme without message recovery.

10. A method for verifying a public key digital signature against an individual message and a public key in an electronic system, comprising:

    a) parsing said public key digital signature and retrieving its signature data,

    b) ascertaining that said signature data comprises a stated signature value and a stated sibling value-and-position sequence,

    c) computing a hash tree branch comprising a leaf node and a root node, said hash tree branch being computed with the value of said individual message and with said stated sibling value-and-position sequence,

d) performing a verification operation on said stated signature value with the value of said root node and with said public key,

whereby a verifier can determine that said public key digital signature was generated from said individual message by a holder of a private key corresponding to said public key.

11. The method of claim 10, wherein

a) said stated signature value comprises a stated cryptographic signature and a stated padding value,

and further including

b) performing said verification operation with said stated padding value added to the value of said root node,

whereby a verifier can verify a signature when using a cryptographic signature scheme without message recovery.

12. The method of claim 10, wherein

a) said stated signature value comprises a stated cryptographic signature, and

b) said verifying step uses a cryptographic signature scheme with message recovery.

13. The method of claim 10, wherein

a) said hash tree branch is computed with a position-dependent hash function.

14. The method of claim 10, further including

a) ascertaining that said signature data comprises a hash tree size,

b) determining a tree representative of a tree family, said tree representative having said hash tree size, and

c) determining whether or not the shape of said hash tree branch is a valid branch of said tree representative,

whereby a verifier can determine that said public key digital signature was not generated as a tree extension.

15. The method of claim 10, further including

a) ascertaining that said signature data comprises a salt value,

and wherein

b) the hash function used to compute said hash tree branch is a salted hash function that incorporates said salt value.

whereby a verifier can have an assurance that said public key digital signature was not generated as a tree extension.

16. The method of claim 10, wherein

a) the value of the leaf of said hash tree branch is taken as the result of a hash function applied to the value of said individual message,

whereby a verifier can have an assurance that said public key digital signature was not generated as a tree extension.

17. A signature data structure embodied in a computer-readable medium, comprising:

a) a value-and-position sequence, said value-and-position sequence comprising a sibling sequence for a branch from a leaf to the root of a hash tree, and

b) a public key signature,

whereby a signature maker has the ability to store and to transmit said signature data structure comprising a public key digital signature.

18. The signature data structure of claim 17, further including

a) a padding value,

whereby a verifier can verify a signature when using a cryptographic signature scheme without message recovery.

19. The signature data structure of claim 17, further including

a) a tree size value,

whereby a verifier can determine that said public key digital signature was not generated as a tree extension.

20. The signature data structure of claim 17, further including

a) a salt value,

whereby a verifier can verify a signature when said signature was generated with a salted hash function.